

16925 U.S. PRO
09/670119
09/26/00

NEP/tf
Washington, D.C. 20006
Telephone (202) 721-8200
September 26, 2000

1c925 U.S. PTO
09/670119
09/26/00

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

1999年 9月30日

出 願 番 号
Application Number:

平成11年特許願第280075号

出 願 人
Applicant (s):

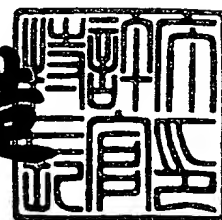
松下電器産業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 7月21日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2000-3056189

【書類名】 特許願

【整理番号】 2032410354

【提出日】 平成11年 9月30日

【あて先】 特許庁長官 殿

【国際特許分類】 G11B 19/00

【発明者】

 【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

 【氏名】 弓場 隆司

【発明者】

 【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

 【氏名】 石原 秀志

【発明者】

 【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

 【氏名】 福島 能久

【発明者】

 【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

 【氏名】 館林 誠

【発明者】

 【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

 【氏名】 横田 薫

【特許出願人】

 【識別番号】 000005821

 【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100077931

【弁理士】

【氏名又は名称】 前田 弘

【選任した代理人】

【識別番号】 100094134

【弁理士】

【氏名又は名称】 小山 廣毅

【手数料の表示】

【予納台帳番号】 014409

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9601026

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報記録媒体、情報再生方法および情報再生装置

【特許請求の範囲】

【請求項 1】 コンテンツ情報が記録された情報記録媒体であって、
リードイン領域と、
データ記録領域とを有し、
前記リードイン領域には第 1 の暗号化鍵情報が記録され、
前記データ記録領域には少なくとも第 2 の暗号化鍵情報と前記コンテンツ情報
とが記録され、

前記データ記録領域に記録された前記コンテンツ情報はその一部がスクラン
ブルされて記録されており、

このスクランブルされて記録されたコンテンツ情報は、前記第 2 の暗号化鍵情
報を前記コンテンツ情報のうちスクランブルされていない部分を用いて変換する
ことによって得られるスクランブル鍵情報を用いて、スクランブルされている
ことを特徴とする情報記録媒体。

【請求項 2】 請求項 1 に記載の情報記録媒体において、
前記データ記録領域は複数のセクタに分割されており、
前記セクタのそれぞれは、セクタを識別する情報を記録するセクタヘッダ領域
と、前記コンテンツ情報を記録するメインデータ領域とを有し、
前記セクタヘッダ領域には前記第 2 の暗号化鍵情報が記録され、
前記メインデータ領域に記録された前記コンテンツ情報はその一部がスクラン
ブルされて記録されており、

このスクランブルされて記録されたコンテンツ情報は、前記第 2 の暗号化鍵情
報をセクタ毎の前記コンテンツ情報のうちスクランブルされていない部分を用い
て変換することによって得られるスクランブル鍵情報を用いて、スクランブルさ
れている
ことを特徴とする情報記録媒体。

【請求項 3】 請求項 1 又は 2 に記載の情報記録媒体において、
前記スクランブル鍵情報を作成する際に用いられる前記コンテンツ情報のうち

スクランブルされていない部分には、少なくともコピー制御情報を含むことを特徴とする情報記録媒体。

【請求項4】 請求項2に記載の情報記録媒体において、
前記スクランブル鍵情報を作成する際に用いられる前記コンテンツ情報のうちスクランブルされていない部分には、少なくとも、
コピー制御情報と、
セクタ毎に変化するコンテンツ情報の一部とを含む
ことを特徴とする情報記録媒体。

【請求項5】 請求項2に記載の情報記録媒体において、
前記セクタヘッダに記録される前記第2の暗号化鍵情報は、
前記リードイン領域に記録される前記第1の暗号化鍵情報を用いて暗号化されたものである
ことを特徴とする情報記録媒体。

【請求項6】 リードイン領域とデータ記録領域とを備え、前記リードイン領域には第1の暗号化鍵情報が記録され、前記データ記録領域には少なくとも第2の暗号化鍵情報とコンテンツ情報とが記録され、前記コンテンツ情報はその一部がスクランブルされて記録されている情報記録媒体を再生する情報再生方法であって、

前記リードイン領域に記録された前記第1の暗号化鍵情報を復号し、
この復号結果を用いて前記データ記録領域に記録された前記第2の暗号化鍵情報を復号し、

この復号結果を前記データ記録領域に記録された前記コンテンツ情報のうちスクランブルされていない部分を用いて変換し、

この変換結果を用いてスクランブルされて記録されたコンテンツ情報をデスクランブルする
ことを特徴とする情報再生方法。

【請求項7】 リードイン領域とデータ記録領域とを備え、前記リードイン領域には第1の暗号化鍵情報が記録され、前記データ記録領域には少なくとも第2の暗号化鍵情報とコンテンツ情報とが記録され、前記コンテンツ情報はその一

部がスクランブルされて記録されている情報記録媒体を再生する情報再生装置であって、

前記情報記録媒体のリードイン領域に記録された前記第1の暗号化鍵情報を復号する第1の鍵情報復号手段と、

前記データ記録領域に記録された前記第2の暗号化鍵情報を復号する第2の鍵情報復号手段と、

前記第2の鍵情報復号手段の出力を前記データ記録領域に記録された前記コンテンツ情報のうちスクランブルされていない部分を用いて変換する鍵情報変換手段と、

前記スクランブルされて記録されたコンテンツ情報を前記鍵情報変換手段の出力によりデスクランブルするデスクランブル手段と
を備えたことを特徴とする情報再生装置。

【請求項8】 請求項7に記載の情報再生装置において、

前記コンテンツ情報のうちスクランブルされていない部分には、少なくともコピー制御情報を含む
ことを特徴とする情報再生装置。

【請求項9】 請求項7に記載の情報再生装置において、

前記第2の鍵情報復号手段は、

前記第1の鍵情報復号手段の出力を用いて、前記第2の暗号化鍵情報を復号する
ことを特徴とする情報再生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、映像情報や音声情報等を記録する情報記録媒体と、情報記録媒体に記録された情報を再生する情報再生装置に関するものである。

【0002】

【従来の技術】

近年、音声情報の記録媒体としてコンパクトテープやアナログレコードなどの

アナログ信号で記録する記録媒体から、CD (Compact Disc) やMD (Mini Disc) などのデジタル信号で記録する記録媒体が主流になってきている。また、映像信号の記録媒体もMPEG (moving picture coding experts group) 1と呼ばれる圧縮方式で圧縮された映像信号をCDに記録するVideo-CD、さらには4.7GBの大容量を有する光ディスクにMPEG 2と呼ばれる高品位な圧縮方式による圧縮映像信号を記録するDVD (Digital Video Disc) などのデジタル記録媒体が開発され、映像・音声の記録媒体として商品化されている。

【0003】

従来の情報再生装置の構成について簡単に説明する。図4は従来の情報再生装置の構成図である。図4において、400は光ディスクから読み出したデータを誤り訂正処理や伸長処理を施して所望の映像信号や音声信号を出力する情報再生装置全体を示している。201は光ディスク、202は光ディスク201を後述するサーボ制御手段211により回転させるスピンドルモータ、203はレーザーを駆動して光ディスク201を照射し反射光を受光する光学ヘッド、204は光学ヘッド203からの出力信号を増幅するヘッドアンプ、205はAGC (auto gain control)、イコライズ、データリズ、PLL (phase-locked-loop) の機能を有するアナログ処理部、206は再生データを復調し、誤り訂正処理などを行う光ディスクコントローラ、207は光ディスクコントローラ206でエラー訂正に用いる誤り訂正用メモリ、209は圧縮されている映像・音声データに対して伸長処理を施し、音声信号と映像信号として出力するAVデコーダ (オーディオ・ビデオデコード手段)、210は映像・音声データの伸長処理に用いられるAV信号処理用メモリ (伸張用バッファメモリ)、211はフォーカス、トラッキングなどのサーボ制御を行うサーボ制御手段である。412はCPUであり、CPUバス213を介してアナログ処理部205、光ディスクコントローラ206、AVデコーダ209、サーボ制御手段211を制御し、装置全体の動作を制御する。

【0004】

従来の情報再生装置の動作について、図4を用いて簡単に説明する。CPU 412は所定のシーケンスで、光ディスク201からデータを読み出し、エラー訂

正が施されたデータを誤り訂正用メモリ207に格納されるように制御する。この時、CPU412は誤り訂正用メモリ207に格納されたデータのうち、制御情報やデータの識別情報を読み出し、サーボ制御手段211を制御したり、AVデコーダ209の制御を行ったりして、ビデオデータやオーディオデータの再生を行っている。

【0005】

一方、パーソナルコンピュータ（以下PC）の高性能化やハードディスクの大容量化に伴い、PCのアプリケーションプログラムも大容量化が進んでいる。DVDはその大容量の特徴を活かし映像・音声の記録媒体だけでなく、PCのアプリケーションソフトウェア等の頒布媒体としても活用されており、PCの周辺装置としてのDVDドライブの普及が急激に進んでいる。さらに、PC用としてMPEGの伸長機能を備えたAVデコーダカードや、PCのメインプロセッサのソフトウェア処理によりMPEG伸長機能を行うプログラムなども商品化されている。

【0006】

しかしながら、DVDドライブとAVデコーダカードを用いてPCでDVDの映像・音声のデータを再生するシステムでは、これらの装置間は一般的なコンピュータバスの通信路により接続されていることから、通信路を介して伝送されるデータの不正コピーや、データを改竄されて頒布されるなどの行為が行われ、著作権者の権利を保護することが極めて困難となるという課題がある。

【0007】

この課題に対応するために、著作権を有するデータを暗号化して記録することが提案されている。特開平7-249264号公報の図3に開示されたCD-ROMでは、暗号化されたデータセクタとは異なるセクタのメインデータ領域に暗号鍵を記録する方式が提案されている。本従来例では、記録時に暗号化されたデータとその暗号鍵をCD-ROMに記録し、再生時にはパーソナルコンピュータから再生装置に対して暗号鍵の読み出し命令を行った後に暗号化データを読み出して、先に読み出した暗号鍵を用いて復号することにより、データ再生を実現するというものである。

【0008】

【発明が解決しようとする課題】

しかしながら、特開平7-249264号公報に開示された従来例では、暗号鍵が一般的な読み出し命令（Readコマンド）によって読み出すことができるセクタのメインデータ領域に記録されているため、暗号鍵を一般のパーソナルコンピュータから容易に読み出すことができる。

【0009】

従って、暗号鍵と暗号化データをユーザが読み出すことができるために、暗号の解読を行われる危険性が高いという課題があるとともに、暗号鍵と暗号化データを例えばハードディスクにコピーされて不正な複製を作成される可能性があるという課題がある。

【0010】

また、セクタのメインデータ領域全てを暗号化して記録されているために、DVDプレイヤーの様に、セクタのメインデータ中に含まれる、コンテンツの識別情報やコンテンツのコピー制御情報等が含まれるコンテンツ制御情報を、DVDプレイヤーの制御のためにCPUで読み込もうとすると、一度暗号化されたデータを復号してからでないと正しい情報を得ることはできない。

【0011】

上記した課題に対して、コンテンツ制御情報が含まれる領域を平文のまま記録してしまうと、コピー制御情報が不正に改竄された場合、不正な再生が行われることになる。

【0012】

本発明は上記問題点に鑑み、デスクランブル処理に用いる鍵情報を容易に読み出されないことを実現するためのデータ構造を有する情報記録媒体を提供し、かつプレイヤーにおいて、プレイヤーを制御するCPUが容易にコピー制御情報等を読み込み、プレイヤーの制御を行え、かつコピー制御情報等が不正に改竄されても、正常に再生できない情報記録媒体、情報再生方法および情報再生装置を提供することを目的とする。

【0013】

【課題を解決するための手段】

前記課題を解決するため、請求項 1 の発明が講じた手段は、コンテンツ情報が記録された情報記録媒体であって、リードイン領域と、データ記録領域とを有し、前記リードイン領域には第 1 の暗号化鍵情報が記録され、前記データ記録領域には少なくとも第 2 の暗号化鍵情報と前記コンテンツ情報とが記録され、前記データ記録領域に記録された前記コンテンツ情報はその一部がスクランブルされて記録されており、このスクランブルされて記録されたコンテンツ情報は、前記第 2 の暗号化鍵情報を前記コンテンツ情報のうちスクランブルされていない部分を用いて変換することによって得られるスクランブル鍵情報を用いて、スクランブルされているものである。

【0014】

また、請求項 2 の発明は、請求項 1 に記載の情報記録媒体において、前記データ記録領域は複数のセクタに分割されており、前記セクタのそれぞれは、セクタを識別する情報を記録するセクタヘッダ領域と、前記コンテンツ情報を記録するメインデータ領域とを有し、前記セクタヘッダ領域には前記第 2 の暗号化鍵情報が記録され、前記メインデータ領域に記録された前記コンテンツ情報はその一部がスクランブルされて記録されており、このスクランブルされて記録されたコンテンツ情報は、前記第 2 の暗号化鍵情報をセクタ毎の前記コンテンツ情報のうちスクランブルされていない部分を用いて変換することによって得られるスクランブル鍵情報を用いて、スクランブルされているものである。

【0015】

さらに、請求項 3 の発明は、請求項 1 又は 2 に記載の情報記録媒体において、前記スクランブル鍵情報を作成する際に用いられるスクランブルされていないコンテンツ情報の一部には、少なくともコピー制御情報を含むものである。

【0016】

また、請求項 4 の発明は、請求項 2 に記載の情報記録媒体において、前記スクランブル鍵情報を作成する際に用いられる前記コンテンツ情報のうちスクランブルされていない部分には、少なくとも、コピー制御情報と、セクタ毎に変化するコンテンツ情報の一部とを含むものである。

【0017】

また、請求項5の発明では、請求項2に記載の情報記録媒体において、前記セクタヘッダに記録される前記第2の暗号化鍵情報は、前記リードイン領域に記録される前記第1の暗号化鍵情報を用いて暗号化されたものである。

【0018】

また、請求項6の発明は、リードイン領域とデータ記録領域とを備え、前記リードイン領域には第1の暗号化鍵情報が記録され、前記データ記録領域には少なくとも第2の暗号化鍵情報とコンテンツ情報とが記録され、前記コンテンツ情報はその一部がスクランブルされて記録されている情報記録媒体を再生する情報再生方法であって、前記リードイン領域に記録された前記第1の暗号化鍵情報を復号し、この復号結果を用いて前記データ記録領域に記録された前記第2の暗号化鍵情報を復号し、この復号結果を前記データ記録領域に記録された前記コンテンツ情報のうちスクランブルされていない部分を用いて変換し、この変換結果を用いてスクランブルされて記録されたコンテンツ情報をデスクランブルするものである。

【0019】

また、請求項7の発明は、リードイン領域とデータ記録領域とを備え、前記リードイン領域には第1の暗号化鍵情報が記録され、前記データ記録領域には少なくとも第2の暗号化鍵情報とコンテンツ情報とが記録され、前記コンテンツ情報はその一部がスクランブルされて記録されている情報記録媒体を再生する情報再生装置であって、前記情報記録媒体のリードイン領域に記録された前記第1の暗号化鍵情報を復号する第1の鍵情報復号手段と、前記データ記録領域に記録された前記第2の暗号化鍵情報を復号する第2の鍵情報復号手段と、前記第2の鍵情報復号手段の出力を前記データ記録領域に記録された前記コンテンツ情報のうちスクランブルされていない部分を用いて変換する鍵情報変換手段と、前記スクランブルされて記録されたコンテンツ情報を前記鍵情報変換手段の出力によりデスクランブルするデスクランブル手段とを備えたものである。

【0020】

また、請求項8の発明は、請求項7に記載の情報再生装置において、前記コン

テンツ情報のうちスクランブルされていない部分には、少なくともコピー制御情報を含むものである。

【0021】

また、請求項9の発明は、請求項7に記載の情報再生装置において、前記第2の鍵情報復号手段は、前記第1の鍵情報復号手段の出力を用いて、前記第2の暗号化鍵情報を復号するものである。

【0022】

本発明によると、情報記録媒体のデータ記録領域にスクランブル処理を施して記録する際に、情報記録媒体に記録された鍵情報をコピー制御情報やデータの一部を用いて変換してスクランブル用鍵情報として生成するので、コピー制御情報にスクランブル処理を施さなくても、不正に改竄された場合にはスクランブル鍵情報が異なるものとなり、正常な再生ができなくなる。またデータの一部を用いることにより、セクタ毎にスクランブル用鍵情報が異なるので、不正な攻撃に対して強度が強くなる。

【0023】

【発明の実施の形態】

以下、本発明の一実施形態に係る情報記録媒体及び情報再生装置に関して、図面を参照しながら説明する。以下、情報記録媒体として光ディスク（DVD）を例に取り説明する。

【0024】

図1は本実施形態における情報記録媒体のデータ構造を示す説明図である。図1（a）はディスク全体の情報記録領域の構造を示しており、制御情報が記録されるリードイン領域100と、コンテンツ制御情報とコンテンツデータからなるコンテンツ情報が記録されるデータ記録領域101、リードアウト領域102とから構成されている。

【0025】

リードイン領域100には、情報再生装置が光ディスクを再生するために必要とする情報が記録されるコントロールデータ領域110が含まれており、コントロールデータ領域は、図1（b）で示すように物理情報セクタ111やスクラン

ブル情報セクタ 112 等を含んでいる。物理情報セクタ 111 にはディスク径、ディスク構造、記録密度などのディスクの物理情報が記録されており、スクランブル情報セクタ 112 には第 1 の鍵情報に暗号を施した第 1 の暗号化鍵情報が記録されている。

【0026】

データ記録領域には、圧縮された映画や音楽等のコンテンツ情報がファイルとして記録されている。図 1 (a) に示すように、著作権を保護すべきコンテンツはスクランブルされてスクランブルファイル 120 として記録され、著作権がフリーなコンテンツはスクランブルされずに、非スクランブルファイル 130 として記録されている。

【0027】

データ記録領域はセクタと呼ばれる単位で区切られている。図 1 (c) 及び (d) に示すように、スクランブルファイル 120 はスクランブルセクタ、非スクランブルファイル 130 は非スクランブルセクタを有している。図 1 (e) 及び (f) に示すように、スクランブルセクタ、非スクランブルセクタは、セクタを識別するためのアドレス情報等が記録される 12 バイトのセクタヘッダ領域 121、131 と、コンテンツ情報が記録される 2048 バイトのメインデータ領域 122、132 を有している。スクランブルセクタのセクタヘッダ領域 121 には、前述のアドレス情報に加え、スクランブルフラグや第 2 の鍵情報に暗号を施した第 2 の暗号化鍵情報 123 等が記録されている。非スクランブルセクタのセクタヘッダ領域 131 においては、スクランブルセクタのセクタヘッダ領域 121 で第 2 の暗号化鍵情報 123 が格納される領域に相当する領域はリザーブ状態とされ、この領域全てに“0”が記録される。

【0028】

セクタヘッダ領域 121、131 に記録されるスクランブルフラグはそのセクタのメインデータ領域の所定領域がスクランブルされているか否かを示すフラグであり、スクランブルデータが記録されているスクランブルセクタの場合にはスクランブルフラグは“1”、非スクランブルセクタの場合にはスクランブルフラグは“0”が記録される。

【0029】

セクタヘッダ領域に記録される第2の暗号化鍵情報123は、リードイン領域100のスクランブル情報セクタ112に記録されている第1の暗号化鍵情報を復号した結果を鍵として復号処理され、復号された第2の鍵情報はメインデータのデスクランブル処理に用いられる情報となる。

【0030】

また、図1(e)に示すように、スクランブルセクタのメインデータ領域122は、メインデータ領域の全てをスクランブルして記録するものではなく、図1(g)に示すようにコンテンツ制御情報124が含まれる領域やコンテンツデータの一部を除いてスクランブルされている。コピー制御情報126には、コンテンツのコピー制限回数や再生時のダウンサンプリング制御等の情報が記載されている。このスクランブルされたコンテンツデータは、第2の暗号化鍵情報を、コンテンツ制御情報124に含まれるコピー制御情報及び圧縮されたコンテンツの一部(図1(g)の参照データ127)を用いて変換して得られるスクランブル鍵情報により、所定領域のデータをスクランブルされて記録されている。

【0031】

以上の様に、構成された情報記録媒体を用いた情報再生装置の実施の形態について、図を用いて説明する。

【0032】

図2は、本実施形態の情報再生装置の全体を示す構成図である。200は光ディスク201から読み出したデータをデスクランブル処理や伸長処理を施して所望の映像信号や音声信号を出力する情報再生装置全体を示している。図4に示した従来例における構成要素と同じものには同じ番号を付与している。

【0033】

201は図1で示したデータ構造を持つ光ディスク、202は光ディスク201を後述するサーボ制御手段211により回転させるスピンドルモータ、203はレーザーを駆動して光ディスク201を照射し反射光を受光する光学ヘッド、204は光学ヘッド203からの出力信号を増幅するヘッドアンプ、205はA/GC、イコライズ、データライズ、PLLの機能を有するアナログ処理部、20

6は再生データを復調し、誤り訂正処理などを行う光ディスクコントローラ、207は光ディスクコントローラ206でエラー訂正に用いる誤り訂正用メモリ、208はスクランブルされて記録されている情報にデスクランブル処理を施すデスクランブル回路、209は圧縮されている映像・音声データに対して伸長処理を施し、音声信号と映像信号として出力するAVデコーダ（オーディオ・ビデオデコード手段）、210は映像・音声データの伸長処理に用いられるAV信号処理用メモリ、211はフォーカス、トラッキングなどのサーボ制御を行うサーボ制御手段である。212はCPUであり、プログラムROM（図示せず）に格納されたプログラムに従って、CPUバス213を介してアナログ処理部205、光ディスクコントローラ206、デスクランブル回路208、AVデコーダ209、サーボ制御手段211を制御し、装置全体の動作を制御する。

【0034】

デスクランブル回路208はリードイン領域100のスクランブル情報セクタ112に記録されている第1の暗号化鍵情報を入力し、第1の暗号化鍵情報を復号するとともに、図1（c）で示した構造を持つセクタデータを入力し、第2の暗号化鍵情報の復号処理及びメインデータのデスクランブル処理を実施するものである。

【0035】

デスクランブル回路208について説明する。図3はデスクランブル回路208の全体構成を示す構成図である。301はCPUバス213を経由してCPU212から設定される復号モード設定情報に応じて、入力されるデータの内部での出力先を選択する第1の信号選択手段、302は第1の暗号化鍵情報の復号に用いる固定鍵を格納する固定鍵情報格納手段、303は第1の信号選択手段301から出力されるセクタデータを入力して、セクタデータのセクタ内の位置に応じて、つまりセクタデータのデータ数をカウントしたカウント値に応じて、出力先を選択する第2の信号選択手段である。

【0036】

また304は第1の鍵情報復号手段であり、第1の信号選択301から出力されるリードイン領域のスクランブル情報セクタ112の第1の暗号化鍵情報に対

して固定鍵情報格納手段 302 から出力される固定鍵情報を用いて復号処理を行い、復号された第 1 の鍵情報を出力するものである。305 は第 2 の鍵情報復号手段であり、第 2 の信号選択手段 303 から出力される第 2 の暗号化鍵情報を入力し、第 1 の鍵情報復号手段 304 から出力される、復号された第 1 の鍵情報を用いて復号処理を行い、復号された第 2 の鍵情報を出力するものである。

【0037】

さらに、310 は、第 2 の鍵情報復号手段 305 から出力される、復号された第 2 の鍵情報を、第 2 の信号選択手段から出力されるコピー制御情報と参照データとを用いて変換し、デスクランブル用鍵情報を出力する鍵情報変換手段であり、復号された第 2 の鍵情報をコピー制御情報を用いて変換する第 1 の鍵変換手段 311 と、第 1 の鍵変換手段 311 の出力を参照データを用いて変換する第 2 の変換手段 312 とを備えている。

【0038】

306 は第 2 の信号選択手段 303 から出力されるメインデータを入力し、鍵情報変換手段 310 から出力されるデスクランブル用鍵情報を用いてデータのデスクランブル処理を施すデータデスクランブル手段、307 はデータデスクランブル手段 310 の出力及び第 2 の信号選択手段 303 の出力のうち、いずれか一つを選択して出力する第 3 の信号選択手段である。

【0039】

以上の様に構成された、本実施形態の情報再生装置の動作について、図 1～3 を参照して説明する。

【0040】

情報再生装置（光ディスク再生装置）200 は電源投入時にディスクが挿入されている場合、又は新たにディスクが挿入された場合には、リードイン領域 100 のスクランブル情報セクタ 112 に記録されている第 1 の暗号化鍵情報の復号処理を行う。CPU 212 はサーボ制御手段 211 を制御して光学ヘッド 203 からリードイン領域 100 のスクランブル情報セクタ 112 の情報を読み出すよう制御する。

【0041】

読み出された信号には、ヘッドアンプ 204、アナログ処理部 205 及び光ディスクコントローラ 206 により、順次増幅、復調処理及びエラー訂正が施される。

【0042】

また、CPU 212 はデスクランブル回路 208 に対して復号モード設定情報として第 1 の暗号化鍵情報を復号するモードを設定し、光ディスクコントローラ 206 からエラー訂正処理後のスクランブル情報セクタ 112 をデスクランブル回路 208 に転送するよう制御する。

【0043】

デスクランブル回路 208 では、第 1 の鍵情報復号モードが設定されることから、入力されたスクランブル情報セクタ 112 のデータは第 1 の信号選択手段 301 により第 1 の鍵情報復号手段 304 に転送され、第 1 の鍵情報復号手段 304 により固定鍵情報格納手段 302 から出力される固定鍵情報を用いて復号処理が施される。なお、この第 1 の鍵情報を復号するモードではデスクランブル回路 208 からはデータは出力されない。

【0044】

続いて装置使用者の操作等に応じてファイルが選択され、映像や音声を再生する動作を説明する。

【0045】

CPU 212 はサーボ制御手段 211 や光学ヘッド 203、アナログ処理部 205、光ディスクコントローラ 206 を制御して光ディスク 201 から所望の情報を読み出し、エラー訂正後のデータを誤り訂正用メモリ 207 に格納する。
また、CPU 212 はデスクランブル回路 208 に対してデータのデスクランブルモードを設定するとともに、AV デコーダ 209 に必要な情報を設定した後に、エラー訂正後のデータを誤り訂正用メモリ 207 からデスクランブル回路 208 に転送する。

【0046】

デスクランブル回路 208 では、データ復号モード設定情報としてデータのデスクランブルモードに設定されることから、第 1 の信号選択手段 301 により、

入力されるセクタデータは、第2の信号選択手段303に転送される。第2の信号選択手段303では、入力されるデータ数をカウントし、カウント値が、セクタヘッダ領域の第2の暗号化鍵情報の位置を示す値の場合には第2の鍵情報復号手段305に、コピー制御情報が含まれるデータ位置を示す値の場合には第1の鍵変換手段311に、参照データの位置を示す値の場合には第2の鍵変換手段312に、メインデータの位置を示す値の場合にはデータデスクランブル手段306及び第3の信号選択手段307にそれぞれ出力するように、入力データを割り振る。

【0047】

第2の鍵情報復号手段305に入力された暗号化された第2の暗号化鍵情報は、第1の鍵情報復号手段105から出力される復号された第1の暗号化鍵情報を鍵として用いて復号される。

【0048】

そして復号された第2の鍵情報は、メインデータに含まれるコピー制御情報を用いて第1の鍵変換手段311で変換され、さらに第1の鍵変換手段311の出力は、メインデータに含まれる参照データにより第2の鍵変換手段312で変換され、デスクランブル用鍵情報が出力される。

【0049】

データデスクランブル手段306に入力されたメインデータは鍵情報変換手段310から出力されるデスクランブル用鍵情報を用いてデスクランブル処理が施され第3の信号選択手段307に出力される。

【0050】

第3の信号選択手段307は、第2の信号選択手段303により選択されたスクランブルフラグを入力し、かつ内部でセクタデータのデータ数をカウントし、この両者の値に応じて選択信号を出力する。この選択信号によって、スクランブルフラグが“1”でかつ、セクタのデータ数のカウント値が非スクランブル領域を示した場合、デスクランブル処理を施されていないメインデータが第3の信号選択手段307から出力され、セクタのデータ数のカウント値がスクランブル領域を示した場合、データデスクランブル手段306の出力が第3の信号選択手

段 307 から出力される。

【0051】

スクランブルフラグが“0”の場合には、セクタデータ数カウント値に関わらず、デスクランブル処理を施されていないメインデータが第3の信号選択手段307から出力される。

【0052】

このようにスクランブルフラグに応じて、デスクランブル処理が施され、デスクランブル回路208から出力されたメインデータは、AVデコーダ209に入力される。AVデコーダ209は、多重化されたオーディオとビデオの圧縮データを分離して、それぞれに伸長処理を施して、映像信号、音声信号として出力する。

【0053】

このように本発明によると、以下の様な効果がある。

【0054】

まず、コピー回数制限や再生時のダウンサンプリング制御などのコンテンツ制御情報124を、情報再生装置(DVDプレイヤー)のシステムコントロール手段(図2のCPU212)が読み込んで、情報再生装置の制御を行う際に、コンテンツ制御情報はスクランブルされずに記録されているので、容易に参照することができる。

【0055】

またコンテンツ制御情報124は、上記の観点からスクランブルされずに記録しているが、不正にコンテンツ制御情報124を改竄した場合、正しくデスクランブル鍵情報を生成することはできないので、不正な再生を防止することができる。

【0056】

さらに、コピー制御情報124を用いて、第2の暗号化鍵情報からスクランブル鍵情報を得る際に、さらにセクタ単位で変化しやすいコンテンツデータを用いているので、コピー制御情報が前述のファイル単位に設定され、かつ第2の暗号化鍵情報も同様にファイル単位で設定されたとしても、スクランブル鍵情報がセ

クタ毎に変わるので、スクランブルによるコンテンツの保護強度を高くすることができる。

【0057】

なお、本実施形態では、情報記録媒体として光ディスクを例として用いたが、磁気ディスク等の他の情報記録媒体であってもよい。

【0058】

【発明の効果】

以上のように本発明の情報記録媒体では、リードイン領域には第1の暗号化鍵情報が記録され、データ記録領域には第2の暗号化鍵情報と、データ及びその一部がスクランブルされたスクランブルデータとが記録され、このスクランブルデータは、第2の暗号化鍵情報からスクランブルされていないデータに含まれるコピー制御情報や参照データを用いて生成されたスクランブル鍵情報を用いてスクランブルされたデータである。従って、装置内の制御のためにスクランブルされずに記録されたコピー制御情報が不正に改竄された場合には、スクランブルする際に用いられたスクランブル鍵情報を得ることができなくなるため、このような不正な行為が行われた場合に正常な再生を防止することが容易にできる。

【0059】

さらに、スクランブルされていないデータを参照データとしてスクランブル鍵情報の生成に用いているので、例えば、第2の暗号化鍵情報やコピー制御情報がファイル単位で設定されたとしてもスクランブル鍵情報はセクタ単位で変化するので、不正な攻撃に対しても強いという効果がある。

【図面の簡単な説明】

【図1】

本実施形態における情報記録媒体のデータ構造を示す説明図である。

【図2】

本実施形態の情報再生装置の全体を示す構成図である。

【図3】

図2の情報再生装置におけるデスクランブル回路の全体構成を示す構成図である。

【図 4】

従来の情報再生装置の構成図である。

【符号の説明】

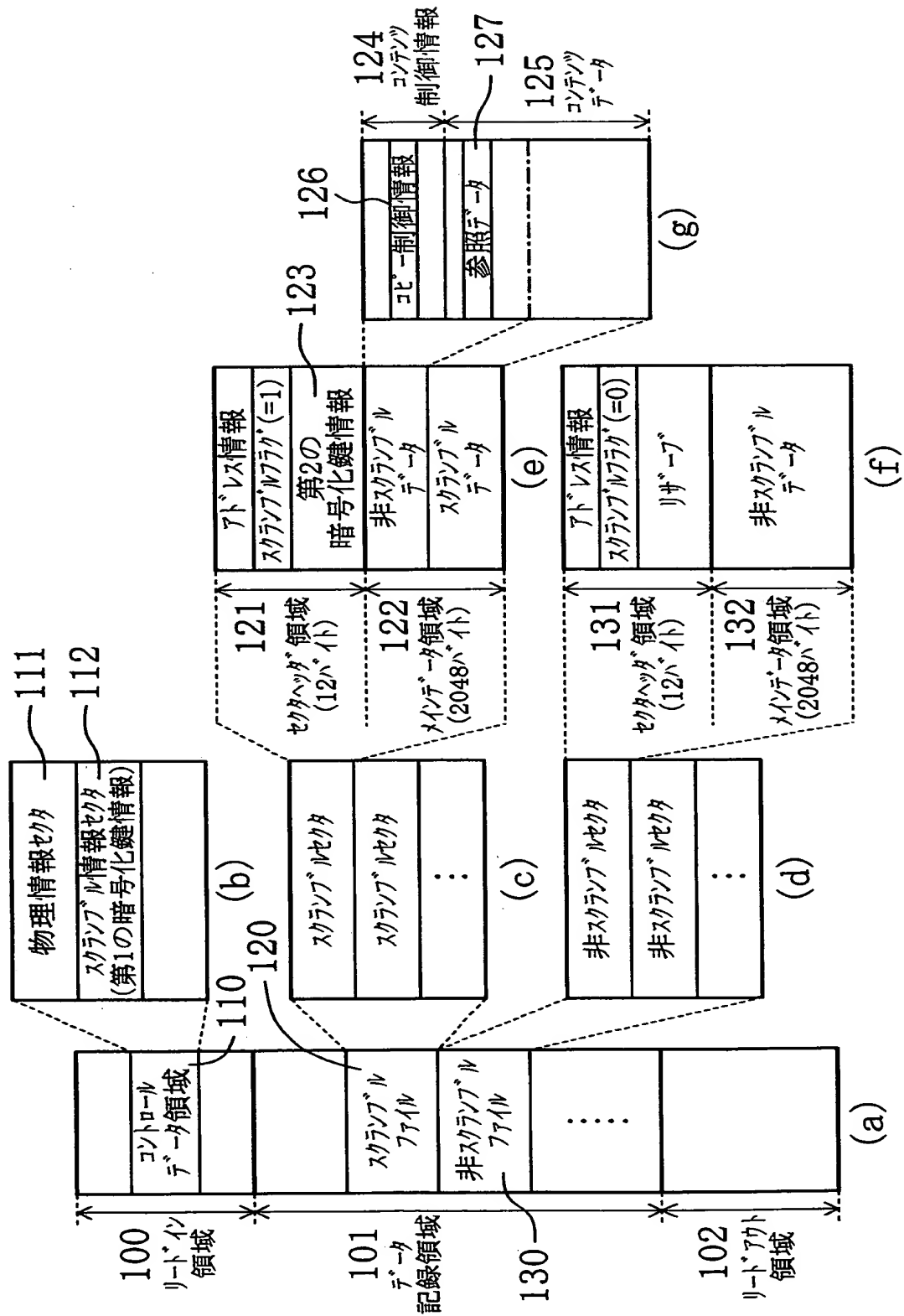
- 1 0 0 リードイン領域
- 1 0 1 データ記録領域
- 1 0 2 リードアウト領域
- 1 1 0 コントロールデータ領域
- 1 1 1 物理情報セクタ
- 1 1 2 スクランブル情報セクタ（第 1 の暗号化鍵情報）
- 1 2 0 スクランブルファイル
- 1 3 0 非スクランブルファイル
- 1 2 1、1 3 1 セクタヘッダ領域
- 1 2 2、1 3 2 メインデータ領域
- 1 2 3 第 2 の暗号化鍵情報
- 1 2 4 コンテンツ制御情報
- 1 2 5 コンテンツデータ
- 1 2 6 コピー制御情報
- 1 2 7 参照データ
- 2 0 0、4 0 0 情報再生装置
- 2 0 1 光ディスク
- 2 0 2 スピンドルモータ
- 2 0 3 光学ヘッド
- 2 0 4 ヘッドアンプ
- 2 0 5 アナログ処理部
- 2 0 6 光ディスクコントローラ
- 2 0 7 誤り訂正用メモリ
- 2 0 8 デスクランブル回路
- 2 0 9 A V デコーダ
- 2 1 0 A V 信号処理用メモリ

- 211 サーボ制御手段
- 212、412 CPU
- 213 CPUバス
- 301 第1の信号選択手段
- 302 固定鍵情報格納手段
- 303 第2の信号選択手段
- 304 第1の鍵情報復号手段
- 305 第2の鍵情報復号手段
- 306 データデスクランブル手段
- 307 第3の信号選択手段
- 310 鍵情報変換手段
- 311 第1の鍵変換手段
- 312 第2の鍵変換手段

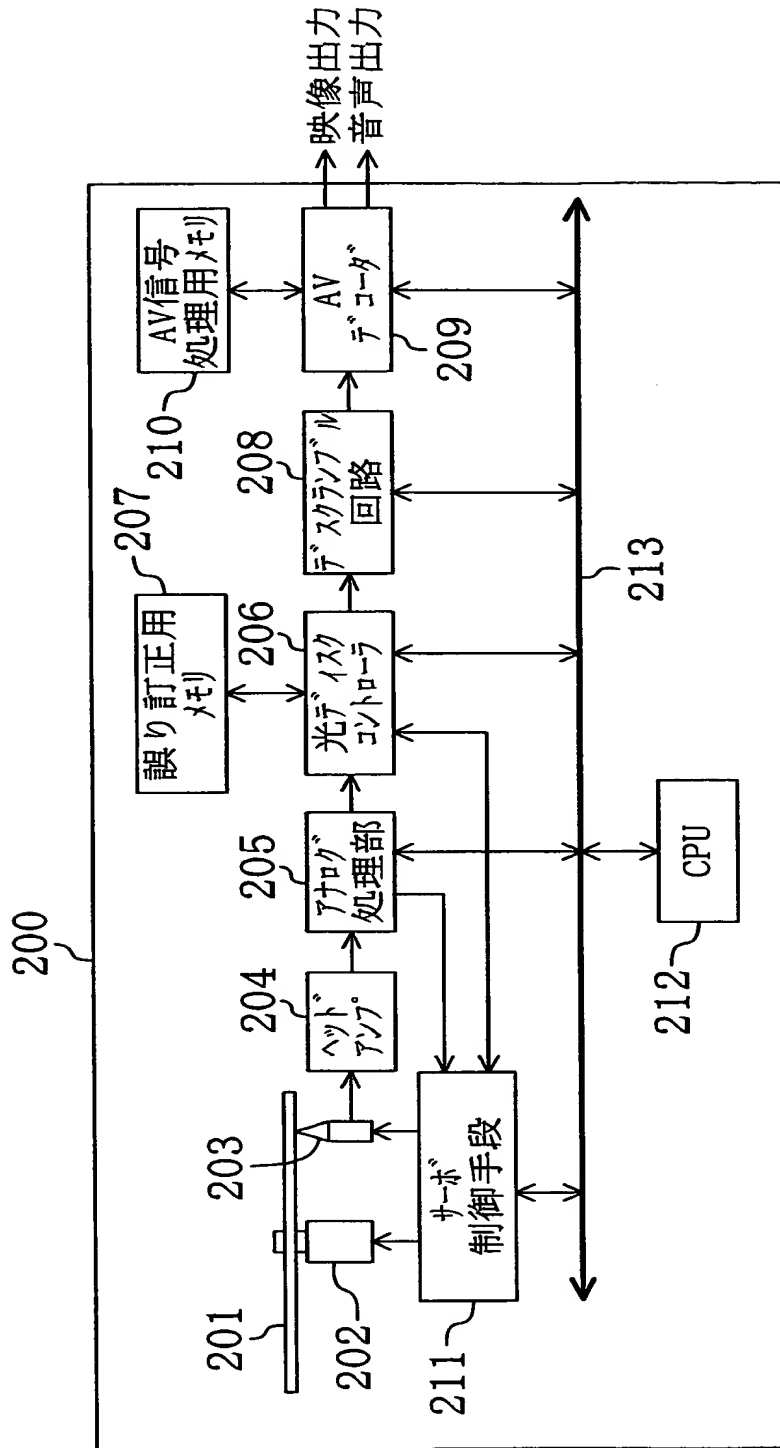
【書類名】

図面

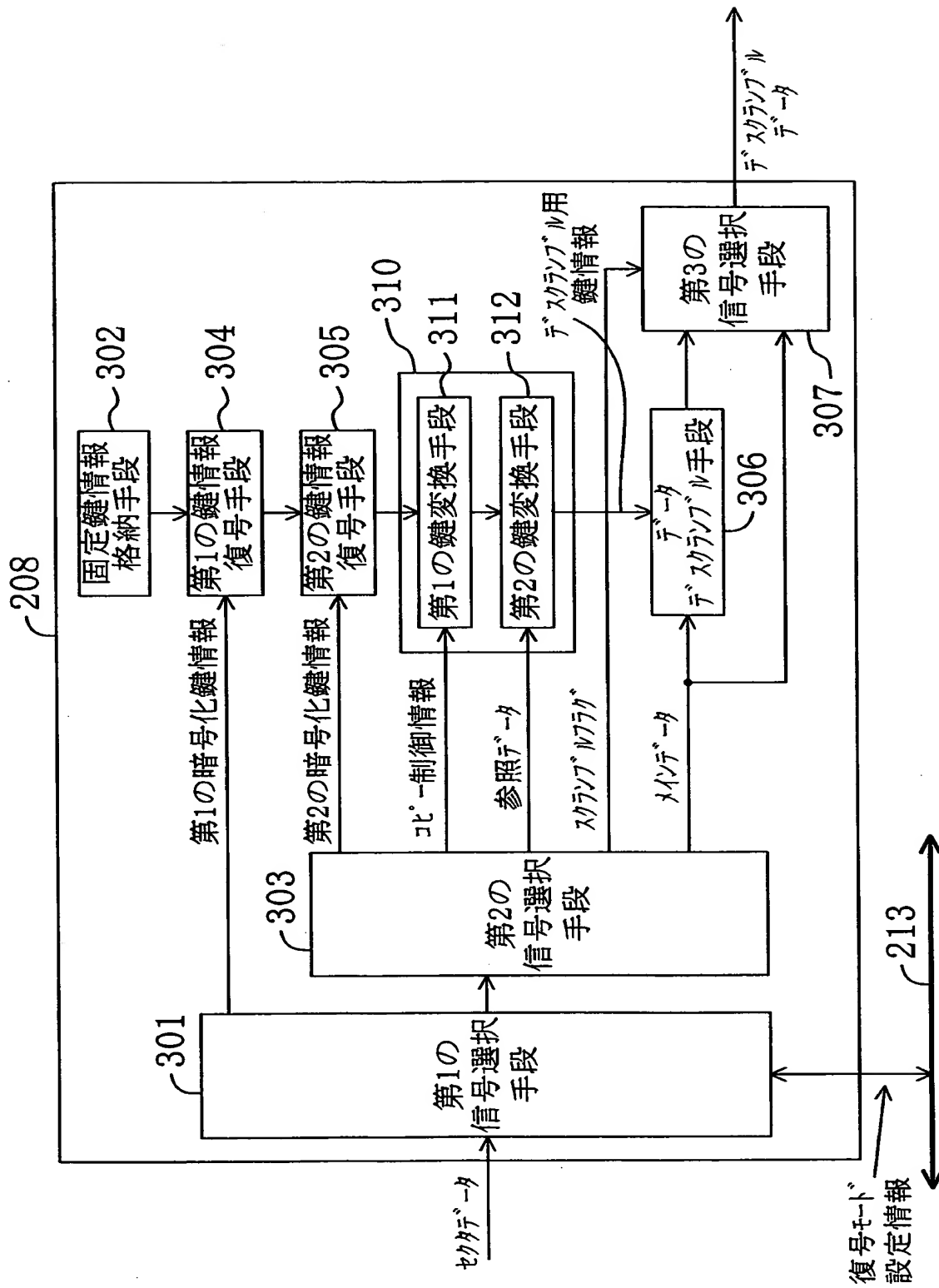
【図 1】



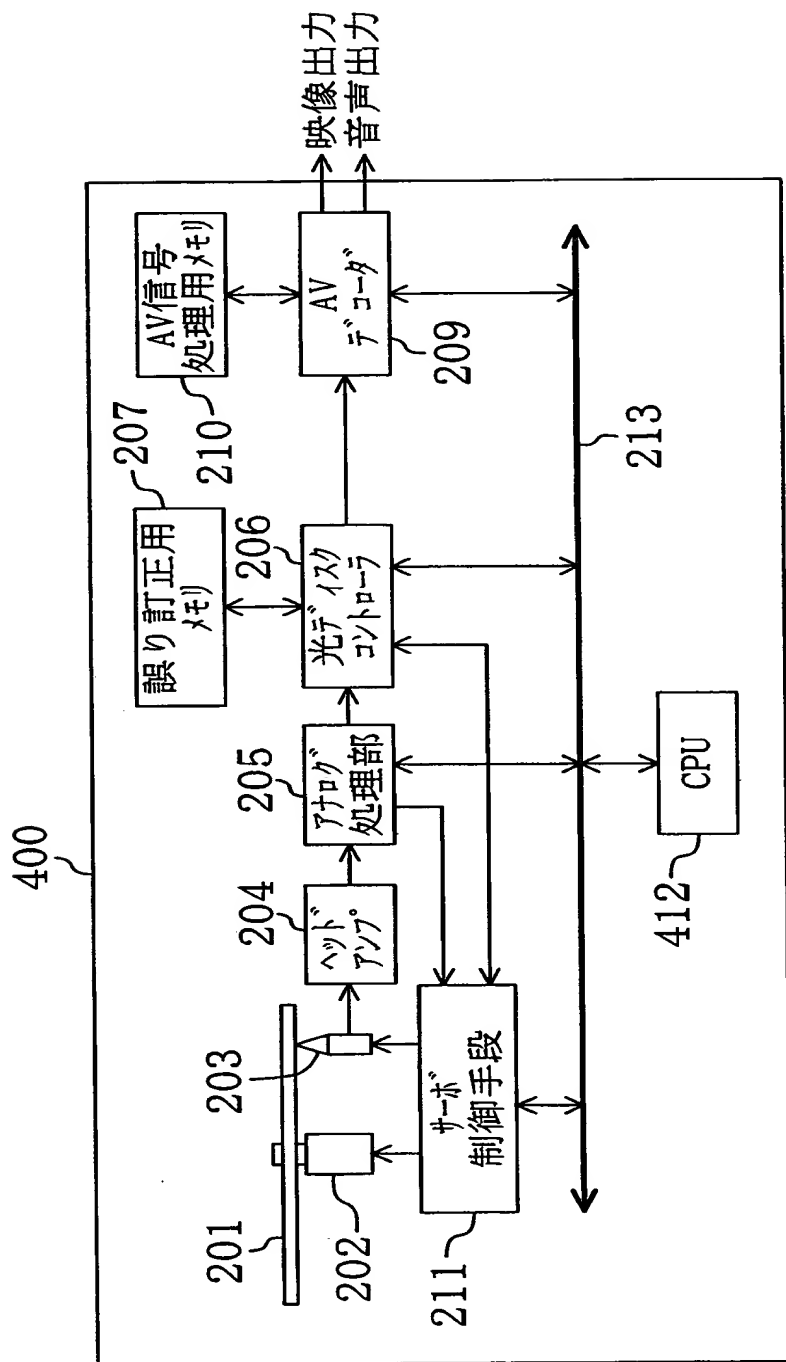
【図 2】



【図 3】



【図 4】



【書類名】 要約書

【要約】

【課題】 コンテンツ情報内のコピー制御情報の不正な改竄に対処できるとともに、コピー制御情報を再生装置で容易に判別できる情報記録媒体を提供する。

【解決手段】 情報記録媒体は、リードイン領域とデータ記録領域とを備え、リードイン領域には第1の暗号化鍵情報が記録され、データ記録領域には第2の暗号化鍵情報とコンテンツ情報とが記録されている。コンテンツ情報は、その一部がスクランブル鍵情報を用いてスクランブルされて記録されている。スクランブル鍵情報は、コンテンツ情報のうちスクランブルされていない部分を用いて前記第2の暗号化鍵情報を変換して得られる。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 大阪府門真市大字門真1006番地

氏 名 松下電器産業株式会社